

ON TAMELY RAMIFIED IWASAWA MODULES FOR THE CYCLOTOMIC \mathbb{Z}_p -EXTENSION OF ABELIAN FIELDS

TSUYOSHI ITOH

ABSTRACT. Let p be an odd prime, and k_∞ the cyclotomic \mathbb{Z}_p -extension of an abelian field k . For a finite set S of rational primes not including p , we will consider the maximal S -ramified abelian pro- p extension $M_S(k_\infty)$ over k_∞ . We shall give a formula of the \mathbb{Z}_p -rank of $\text{Gal}(M_S(k_\infty)/k_\infty)$. In the proof of this formula, we also show that $M_{\{q\}}(k_\infty)/L(k_\infty)$ is a finite extension for every real abelian field k and every rational prime q distinct from p , where $L(k_\infty)$ is the maximal unramified abelian pro- p extension over k_∞ .

1. INTRODUCTION

Let k be an algebraic number field, and p a prime number. We denote by k_∞/k the cyclotomic \mathbb{Z}_p -extension (i.e. the unique \mathbb{Z}_p -extension contained in the field generated by all p -power roots of unity over k). Let S be a finite set of *rational* primes, and $\widetilde{M}_S(k_\infty)$ the maximal pro- p extension of k_∞ unramified outside S (i.e., the primes of k_∞ lying above the primes in S are only allowed to ramify in $\widetilde{M}_S(k_\infty)/k_\infty$).

When S contains p , the structure of $\widetilde{X}_S(k_\infty) = \text{Gal}(\widetilde{M}_S(k_\infty)/k_\infty)$ is already studied (see, e.g., Iwasawa [7], Neukirch-Schmidt-Wingberg [10]). In particular, $\widetilde{X}_S(k_\infty)$ is a free pro- p group under certain conditions.

Recently, the structure of $\widetilde{X}_S(k_\infty)$ for the case that $p \notin S$ is also studied by several authors (Salle [11], Mizusawa-Ozaki [9], ...). In this case, it seems that $\widetilde{X}_S(k_\infty)$ does not have a simple structure. Then, to study $\widetilde{X}_S(k_\infty)$, it is important to study the structure of its abelian quotient. Let $M_S(k_\infty)/k_\infty$ be the maximal abelian pro- p extension unramified outside S . In the present paper, we shall consider $X_S(k_\infty) = \text{Gal}(M_S(k_\infty)/k_\infty)$ for the case that $p \notin S$. Since $\text{Gal}(k_\infty/k)$ acts on $X_S(k_\infty)$, we can use Iwasawa theoretic arguments. We call this $X_S(k_\infty)$ the S -ramified Iwasawa module. (When $p \notin S$, all primes which ramify in $M_S(k_\infty)/k_\infty$ are tamely ramified. We also call these modules “tamely ramified Iwasawa modules”.)

If a \mathbb{Z}_p -module M satisfies $\dim_{\mathbb{Q}_p} M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = r < \infty$, we say that the \mathbb{Z}_p -rank of M is r , and we write $\text{rank}_{\mathbb{Z}_p} M = r$. Our purpose of the present paper is giving a formula of $\text{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ when k is an abelian extension of \mathbb{Q} and p is an odd prime. (In this case, we can show that $X_S(k_\infty)$ is finitely generated over \mathbb{Z}_p .)

We shall give a remark about “giving a formula of $\text{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ ”. Let $L(k_\infty)$ be the maximal unramified pro- p extension of k_∞ . We put $X(k_\infty) = \text{Gal}(L(k_\infty)/k_\infty)$. Then $X(k_\infty)$ is the (usual) Iwasawa module, and $\lambda = \text{rank}_{\mathbb{Z}_p} X(k_\infty)$ is called the Iwasawa λ -invariant. In general, it is hard to write λ explicitly. Since $X(k_\infty)$ is a quotient of $X_S(k_\infty)$, we consider it is sufficient to obtain a formula including λ at the present time. (That is, we will only give a formula of $\text{rank}_{\mathbb{Z}_p} \text{Gal}(M_S(k_\infty)/L(k_\infty))$, actually.) However, for abelian fields, the “plus part” of λ is conjectured to be 0 (Greenberg’s conjecture), and the “minus part” of λ can be computed (at least theoretically) from the Kubota-Leopoldt p -adic L -functions (Stickelberger elements).

We also mention that formulas of $\text{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ are already obtained for several cases. In particular, the \mathbb{Z}_p -rank of the “minus part” of $X_S(k_\infty)$ for CM-fields is already known (see section 2). Salle [11] studied $X_S(k_\infty)$ for the case that k is an imaginary quadratic field and $p = 2$. Moreover, when $k = \mathbb{Q}$, a formula of $\text{rank}_{\mathbb{Z}_p} X_S(\mathbb{Q}_\infty)$ (including the case that $p = 2$) is shown by Mizusawa, Ozaki, and the author [5] (as a corollary, a general formula for imaginary quadratic fields is also given). In the present paper, we shall extend the method given in [5] for abelian fields. The following theorem is crucial to prove the formula of $\text{rank}_{\mathbb{Z}_p} X_S(\mathbb{Q}_\infty)$.

Theorem A. (see [5]) *Let q be a rational prime distinct from p . Then $M_{\{q\}}(\mathbb{Q}_\infty)/\mathbb{Q}_\infty$ is a finite extension.*

At first, we will generalize Theorem A for real abelian fields (under the condition that p is an odd prime).

Theorem 1.1. *Assume that p is odd. Let k be a real abelian field, and q a rational prime distinct from p . Then $M_{\{q\}}(k_\infty)/L(k_\infty)$ is a finite extension.*

We remark that $M_{\{q\}}(k_\infty)/L(k_\infty)$ can be infinite when k is an imaginary abelian field. (For example, see [11], [8], [5], or section 6 of the present paper.) Similar to [5], Theorem 1.1 plays an important role to prove our formula of $\text{rank}_{\mathbb{Z}_p} X_S(k_\infty)$ for abelian fields.

In section 2, we shall state some basic facts, and give some preparations for proving Theorem 1.1. We will prove Theorem 1.1 in sections 3 and 4. In section 5, we shall give a simple remark about a generalization of Theorem 1.1. In section 6, we shall give a formula of $\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)$ for abelian fields (Theorem 6.4). The formula is given as the χ -component version. We also give some examples with applying this formula for some simple cases.

2. PRELIMINARIES

Firstly, we shall recall some basic facts from class field theory. Let p be an odd prime number, and k an algebraic number field. We denote by k_∞/k the cyclotomic \mathbb{Z}_p -extension. For a non-negative integer n , let k_n be the n th layer of k_∞/k (that is, the unique subfield

of k_∞ such that k_n/k is the cyclic extension of degree p^n). Let S be a finite set of rational primes not including p . For an algebraic extension (not necessary finite) \mathcal{K} of \mathbb{Q} , let $M_S(\mathcal{K})$ be the maximal abelian (pro-) p -extension of \mathcal{K} unramified outside S , and $L(\mathcal{K})$ the maximal unramified abelian (pro-) p -extension of \mathcal{K} . For an abelian group G , let \widehat{G} be the p -adic completion of G (that is, $\widehat{G} = \varprojlim G/G^{p^n}$).

As noted in section 1, we shall mainly consider the \mathbb{Z}_p -rank of $\text{Gal}(M_S(k_\infty)/L(k_\infty))$. By class field theory, we have the following exact sequence:

$$\widehat{E_{k_n}} \xrightarrow{\eta_n} \bigoplus_{q \in S} (\widehat{O_{k_n}/q})^\times \rightarrow \text{Gal}(M_S(k_n)/L(k_n)) \rightarrow 0,$$

where E_{k_n} is the group of units of k_n , O_{k_n} is the ring of integers of k_n , and η_n is the natural homomorphism induced from the diagonal embedding. We put $E_\infty = \varprojlim \widehat{E_{k_n}}$, and $R_q = \varprojlim (\widehat{O_{k_n}/q})^\times$, where the projective limits are taken with respect to the natural mappings induced from the norm mapping. Then we obtain the following exact sequence:

$$E_\infty \xrightarrow{\eta_\infty} \bigoplus_{q \in S} R_q \rightarrow \text{Gal}(M_S(k_\infty)/L(k_\infty)) \rightarrow 0.$$

In the cyclotomic \mathbb{Z}_p -extension, all (finite) primes of k are finitely decomposed. Then R_q is a finitely generated \mathbb{Z}_p -module. From this, we also see $\text{Gal}(M_S(k_\infty)/L(k_\infty))$ is finitely generated over \mathbb{Z}_p . On the other hand, the theorem of Ferrero-Washington implies that $\text{Gal}(L(k_\infty)/k_\infty)$ is a finitely generated \mathbb{Z}_p -module, if k is an abelian field. Hence, we see that for every abelian field k , $X_S(k_\infty)$ is finitely generated over \mathbb{Z}_p . (We can see that the \mathbb{Z}_p -rank of $X_S(k_\infty)$ is always finite in general.) Though the computation of the \mathbb{Z}_p -rank of R_q is relatively easy, it seems hard to determine the cokernel of η_∞ directly.

Remark. When the base field k is a CM-field, the minus part of E_∞ is easy to compute (we also able to compute the minus part of R_q). Hence we can obtain a formula of the \mathbb{Z}_p -rank of the minus part of $\text{Gal}(M_S(k_\infty)/L(k_\infty))$. This was already done (see Khare-Wintenberger [8]).

Secondly, we shall give some preparations to prove Theorem 1.1. Let q be a prime number satisfying $q \neq p$. For simplicity, we will write $M_p(\cdot)$, $M_q(\cdot)$, $X_q(\cdot)$ instead of $M_{\{p\}}(\cdot)$, $M_{\{q\}}(\cdot)$, $X_{\{q\}}(\cdot)$, respectively.

Lemma 2.1. *Let k'/k be a finite extension of algebraic number fields. If $\text{Gal}(M_q(k'_\infty)/L(k'_\infty))$ is finite, then $\text{Gal}(M_q(k_\infty)/L(k_\infty))$ is also finite.*

Proof. Let

$$N_n : (\widehat{O_{k'_n}/q})^\times \rightarrow (\widehat{O_{k_n}/q})^\times$$

be the homomorphism induced from the norm mapping. We can see that the order of the cokernel $\text{Coker}(N_n)$ is bounded as $n \rightarrow \infty$. (Proof: Since there are only finitely many

primes in k_∞ lying above q , the p -rank of $(\widehat{O_{k_n}/q})^\times$ is bounded. Moreover, the exponent of $\text{Coker}(N_n)$ is at most $[k' : k]$. Since $\text{Gal}(M_q(k'_n)/L(k'_n))$ (resp. $\text{Gal}(M_q(k_n)/L(k_n))$) is isomorphic to a quotient of $(\widehat{O_{k'_n}/q})^\times$ (resp. $(\widehat{O_{k_n}/q})^\times$), N_n induces the homomorphism $\text{Gal}(M_q(k'_n)/L(k'_n)) \rightarrow \text{Gal}(M_q(k_n)/L(k_n))$. From the above fact, the order of the cokernel is bounded as $n \rightarrow \infty$.

Assume that $\text{Gal}(M_q(k'_\infty)/L(k'_\infty))$ is finite. Then the order of $\text{Gal}(M_q(k'_n)/L(k'_n))$ is bounded as $n \rightarrow \infty$. From the above fact, we see that the order of $\text{Gal}(M_q(k'_n)/L(k'_n))$ is also bounded. Hence $\text{Gal}(M_q(k_\infty)/L(k_\infty))$ is finite. \square

From Lemma 2.1 and the theorem of Kronecker-Weber, we may replace a real abelian field k to the maximal real subfield of a cyclotomic field containing k . For a positive integer d , let μ_d be the set of all d th root of unity, and $\mathbb{Q}(\mu_d)$ the d th cyclotomic field.

Lemma 2.2. *Let f be a positive integer which is prime to p , and m a positive integer. We put $K = \mathbb{Q}(\mu_{fp^m})$ and $k = K^+$ (the maximal real subfield of K). If q does not split in K/k , then $M_q(k_\infty) = L(k_\infty)$.*

Proof. Let \mathfrak{q} be an arbitrary prime of k lying above q . It is well known that if \mathfrak{q} does not split in K , then the order of $(O_k/\mathfrak{q})^\times$ is not divisible by p . (Proof: We denote by $k_{\mathfrak{q}}$ the completion of k at \mathfrak{q} . Under the assumption, $k_{\mathfrak{q}}$ does not contain μ_p . By the structure of the group of units in $k_{\mathfrak{q}}$, we obtain the assertion.) Since $\text{Gal}(M_q(k)/L(k))$ is isomorphic to a quotient of $(O_k/\mathfrak{q})^\times$, we see $M_q(k) = L(k)$.

We note that the n th layer k_n of k_∞/k is the maximal real subfield of $\mathbb{Q}(\mu_{fp^{m+n}})$. Hence by using the same argument, we also see $M_q(k_n) = L(k_n)$ for all $n \geq 1$. This implies that $M_q(k_\infty) = L(k_\infty)$. \square

From the above arguments, it is sufficient to prove Theorem 1.1 under the following conditions:

(A) k is the maximal real subfield of $K = \mathbb{Q}(\mu_{fp^m})$, where f and m are positive integers and f is prime to p . Every prime lying above q splits in K/k , and is not decomposed in k_∞/k (the latter can be satisfied by taking m sufficiently large).

3. PROPERTIES OF CERTAIN KUMMER EXTENSIONS

In this section, we shall give some key results to prove Theorem 1.1. Assume that K, k , and q satisfy (A) in section 2. We will construct certain infinite Kummer extensions over K_∞ . We shall use some fundamental results given by Khare-Wintenberger [8].

We define the terms **case NS** and **case S** as follows:

- case NS : every prime lying above p does not split in K/k ,
- case S : every prime lying above p splits in K/k .

Moreover, we use the following notation (in sections 3 and 4):

- J : complex conjugation
- $\mathfrak{q}_1, \dots, \mathfrak{q}_r$: prime ideals of k lying above q
- $\mathfrak{p}_1, \dots, \mathfrak{p}_t$: prime ideals of k lying above p
- $\mathfrak{Q}_i, \mathfrak{Q}_i^J$ ($i = 1, \dots, r$) : prime ideals of K lying above \mathfrak{q}_i
- \mathfrak{P}_j ($j = 1, \dots, t$) : prime ideals of K lying above p (case NS)
- $\mathfrak{P}_j, \mathfrak{P}_j^J$ ($j = 1, \dots, t$) : prime ideals of K lying above p (case S)

Following Greenberg [2], we denote by s the number of primes of k which is lying above p and splits in K . Hence we see that $s = 0$ for the case NS, and $s = t$ for the case S. Note that every prime lying above p are totally ramified in k_∞/k by the assumption on k . Hence s is also the number of primes of k_∞ which is lying above p and splits in K_∞ .

By the assumption, K_∞ contains all p^n th roots of unity. For an element x of K^\times , we define

$$K_\infty(\sqrt[p^\infty]{x}) = \bigcup_{n \geq 1} K_\infty(\sqrt[p^n]{x}).$$

More precisely, $K_\infty(\sqrt[p^\infty]{x})$ is the union of all finite Kummer extensions $K_n(\sqrt[p^n]{x})$ for $n \geq 1$ (note that K_n contains μ_{p^n}). Similarly, for a finitely generated subgroup T of K^\times , we define the extension $K_\infty(\sqrt[p^\infty]{T})/K_\infty$ by adjoining all p^n th roots of the elements contained in T . As noted in [8], $K_\infty(\sqrt[p^\infty]{x}) = K_\infty$ if and only if x is a root of unity.

The following result is helpful to prove the results stated in this section.

Theorem B. (see Khare-Wintenberger [8]) *Let T be a finitely generated subgroup of K^\times , and S a finite set of (finite) primes of K . Let \mathcal{I} be the subgroup of $\text{Gal}(K_\infty(\sqrt[p^\infty]{T})/K_\infty)$ generated by the inertia subgroups for the primes in S . For a prime \mathfrak{r} contained in S , let $K_{\mathfrak{r}}$ be the completion of K at \mathfrak{r} . We denote by \mathcal{T} be the closure of the diagonal image of T in $\prod_{\mathfrak{r} \in S} \widehat{K_{\mathfrak{r}}^\times}$. (Recall that $\widehat{K_{\mathfrak{r}}^\times}$ is the p -adic completion of $K_{\mathfrak{r}}^\times$.) Then $\text{rank}_{\mathbb{Z}_p} \mathcal{I} = \text{rank}_{\mathbb{Z}_p} \mathcal{T}$.*

We shall construct several Kummer extensions unramified outside $\{p, q\}$ over K_∞ by following the method given in [5]. (See also Greenberg [3].) Let k^D be the decomposition field of K/\mathbb{Q} for q . By the assumption, k^D is an imaginary abelian field and $[k^D : \mathbb{Q}] = 2r$. Let $Q_1, \dots, Q_r, Q_1^J, \dots, Q_r^J$ be the primes of k^D lying below $\mathfrak{Q}_1, \dots, \mathfrak{Q}_r, \mathfrak{Q}_1^J, \dots, \mathfrak{Q}_r^J$ respectively. We can take a positive integer h such that

- Q_1^h is a principal ideal generated by α_1 , and
- $\alpha_1 - 1 \in P$ for every prime ideal P of k^D lying above p .

We note that Q_1^σ ($\sigma \in \text{Gal}(k^D/\mathbb{Q})$) is the complete set of primes in k^D lying above q , and $(Q_1^\sigma)^h = (\alpha_1^\sigma)$. We write all conjugates of α_1 for $\text{Gal}(k^D/\mathbb{Q})$ as the following:

$$\alpha_1, \alpha_2, \dots, \alpha_r, \alpha_1^J, \alpha_2^J, \dots, \alpha_r^J$$

(these are distinct elements because q splits completely in k^D). Moreover, we put $\beta_i = \alpha_i/\alpha_i^J$ for $i = 1, \dots, r$.

For the case S (i.e. p splits in K/k), we define $\rho_1, \dots, \rho_t \in K^\times$ as follows. We can take an integer h' such that $\mathfrak{P}_j^{h'} = (\pi_j)$ for all $j = 1, \dots, t$. We put $\rho_i = \pi_i / \pi_i^J$ for $i = 1, \dots, t$.

Definition. We put

$$T_q = \langle \beta_i \mid i = 1, \dots, r \rangle,$$

which is a subgroup of $(k^D)^\times$ (and hence also a subgroup of K^\times). For the case NS, we put $T = T_q$. For the case S, we put

$$T = \langle \beta_i, \rho_j \mid i = 1, \dots, r, j = 1, \dots, t \rangle.$$

Moreover, we put $N_q = K_\infty(\sqrt[p]{T_q})$ and $N = K_\infty(\sqrt[p]{T})$. (Of course, $N = N_q$ for the case NS.)

Lemma 3.1. (1) N and N_q are abelian extensions over k_∞ . (2) N/K_∞ and N_q/K_∞ are unramified outside $\{p, q\}$. (3) $\text{Gal}(N/K_\infty) \cong \mathbb{Z}_p^{\oplus r+s}$ and $\text{Gal}(N_q/K_\infty) \cong \mathbb{Z}_p^{\oplus r}$. (Recall that $s = 0$ for the case NS, and $s = t$ for the case S.)

Proof. (1) Since J acts on T as -1 , then J acts on $\text{Gal}(N/K_\infty)$ and the action is trivial. This implies that N/k_∞ is an abelian extension. The assertion for N_q follows similarly.

(2) Note that all elements contained in T (resp. T_q) is $\{p, q\}$ -units. Hence N/K_∞ (resp. N_q/K_∞) is unramified outside $\{p, q\}$.

(3) We shall show the assertion for N/K_∞ with the case S (hence $r + s = r + t$). The rest cases can be shown quite similarly. We claim that T is a free \mathbb{Z} -module of rank $r + s$. Since T is generated by the (non-torsion) $r + t$ elements

$$\beta_1, \beta_2, \dots, \beta_r, \rho_1, \rho_2, \dots, \rho_t,$$

it is sufficient to show that there is no relation for these generators. Assume that there are integers a_i ($i = 1, \dots, r + t$) which satisfy

$$\beta_1^{a_1} \beta_2^{a_2} \dots \beta_r^{a_r} \rho_1^{a_{r+1}} \rho_2^{a_{r+2}} \dots \rho_t^{a_{r+t}} = 1,$$

and $a_i \neq 0$ with some i . By using the prime ideal factorization, we see that there are integers b_i ($i = 1, \dots, r + t$)

$$\varpi_1^{b_1} \dots \varpi_r^{b_r} \mathfrak{P}_1^{b_{r+1}} \dots \mathfrak{P}_t^{b_{r+t}} = (\varpi_1^J)^{b_1} \dots (\varpi_r^J)^{b_r} (\mathfrak{P}_1^J)^{b_{r+1}} \dots (\mathfrak{P}_t^J)^{b_{r+t}},$$

and satisfying $b_i \neq 0$ with some i . Since all prime ideals appeared the above equation are distinct, it is a contradiction. Then the claim for the case S follows. The claim for the case NS can be shown by using the same method.

Let \widehat{T} be the closure of T in \widehat{K}^\times . Then \mathbb{Z}_p -rank of T is $r + s$. As noted in [8] (see *Remarks* after the proof of [8, Lemma 2.2]), this fact implies that $\text{rank}_{\mathbb{Z}_p} \text{Gal}(N/K_\infty) = r + s$. Since $\text{Gal}(N/K_\infty)$ is generated by $r + s$ elements, we obtain the isomorphism $\text{Gal}(N/K_\infty) \cong \mathbb{Z}_p^{\oplus r+s}$. The assertion for $\text{Gal}(N_q/K_\infty)$ can be proven quite similarly. \square

For a prime \mathfrak{r} of K , we define $v_{\mathfrak{r}}$ be the normalized valuation of K with respect to \mathfrak{r} .

Lemma 3.2. (cf. Greenberg [3]) (1) For every $i = 1, \dots, r$, the unique prime lying above \mathfrak{Q}_i is ramified in $K_\infty(\sqrt[p^\infty]{\beta_i})/K_\infty$. (2) $N_q \cap M_p(K_\infty)$ is a finite extension over K_∞ .

Proof. (1) Let $\mathcal{I}_{\mathfrak{Q}_i}$ be the inertia group of $\text{Gal}(K_\infty(\sqrt[p^\infty]{\beta_i})/K_\infty)$ for the unique prime of K_∞ lying above \mathfrak{Q}_i . We denote $K_{\mathfrak{Q}_i}$ the completion of K at \mathfrak{Q}_i . Since $v_{\mathfrak{Q}_i}(\beta_i) \neq 0$, then the image of β_i in $\widehat{K_{\mathfrak{Q}_i}^\times}$ generates non-torsion subgroup (see [8]). By Theorem B, we see that $\text{rank}_{\mathbb{Z}_p} \mathcal{I}_{\mathfrak{Q}_i} = 1$, and then the assertion follows.

(2) This fact is already mentioned in [3] without proof. Let \mathcal{I}_q be the subgroup of $\text{Gal}(N_q/K_\infty)$ generated by the inertia groups of the primes lying above q . At first, we shall show that $\text{rank}_{\mathbb{Z}_p} \mathcal{I}_q = r$.

Let \mathcal{T}_q be the closure of the diagonal image of T_q in $\prod_{j=1}^r \widehat{K_{\mathfrak{Q}_j}^\times}$. Assume that $\text{rank}_{\mathbb{Z}_p} \mathcal{T}_q < r$. Then there are elements a_1, \dots, a_r of \mathbb{Z}_p which satisfies

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in } \widehat{K_{\mathfrak{Q}_j}^\times}$$

for all $j = 1, \dots, r$, and $a_i \neq 0$ with some i . However the fact $v_{\mathfrak{Q}_i}(\beta_i) \neq 0$ implies that $a_i = 0$ for all i . It is a contradiction. Then, $\text{rank}_{\mathbb{Z}_p} \mathcal{I}_q = \text{rank}_{\mathbb{Z}_p} \mathcal{T}_q = r$.

By Lemma 3.1, we see $\text{rank}_{\mathbb{Z}_p} \text{Gal}(N_q/K_\infty) = r$. Hence, we found that \mathcal{I}_q has finite index in $\text{Gal}(N_q/K_\infty)$. Since $M_p(K_\infty)/K_\infty$ is unramified at the primes lying above q , we see that $N_q \cap M_p(K_\infty)/K_\infty$ is a finite extension. \square

Proposition 3.3. Let \mathcal{I}_p be the subgroup of $\text{Gal}(N/K_\infty)$ generated by all inertia groups for the prime lying above p . Then \mathcal{I}_p has finite index in $\text{Gal}(N/K_\infty)$.

Proof. Firstly, we consider the case NS. We assume that p does not split in K/k . Hence $s = 0$, $T = T_q$, $N = N_q$, and there are just t primes in K lying above p . By Theorem B and Lemma 3.1, it is sufficient to show that $\text{rank}_{\mathbb{Z}_p} \mathcal{I}_p = r$. Let \mathcal{T}_q be the closure of the diagonal image of T_q in $\prod_{j=1}^t \widehat{K_{\mathfrak{P}_j}^\times}$. By Theorem B, we see that $\text{rank}_{\mathbb{Z}_p} \mathcal{I}_p = \text{rank}_{\mathbb{Z}_p} \mathcal{T}_q$, hence we shall show $\text{rank}_{\mathbb{Z}_p} \mathcal{T}_p = r$.

Recall that k^D is the decomposition field of K/\mathbb{Q} for q , and T_q is also a subgroup of $(k^D)^\times$. We denote by P_1, \dots, P_u the primes of k^D lying above p (where $u \leq t$). Let \mathcal{T}'_q be the closure of the diagonal image of T_q in $\prod_{j=1}^u \widehat{(k_{P_j}^D)^\times}$.

We claim that $\text{rank}_{\mathbb{Z}_p} \mathcal{T}'_q = \text{rank}_{\mathbb{Z}_p} \mathcal{T}_q$. By the definition of T_q , every element x of T_q satisfies $x - 1 \in P_h$ for all $h = 1, \dots, u$. Let $\mathcal{U}_{P_h}^1$ be the group of principal units of $k_{P_h}^D$. We see that \mathcal{T}'_q is contained in $\prod_{h=1}^u \mathcal{U}_{P_h}^1$. Let ι be the homomorphism

$$\prod_{h=1}^u \mathcal{U}_{P_h}^1 \rightarrow \prod_{j=1}^t \mathcal{U}_{\mathfrak{P}_j}^1$$

induced from the diagonal embedding $\mathcal{U}_{P_h}^1 \rightarrow \prod_{\mathfrak{P}|p_h} \mathcal{U}_{\mathfrak{P}}^1$. We can see that ι is injective, and $\iota(\mathcal{T}'_q) = \mathcal{T}_q$. Then the claim follows.

We shall recall the argument given in Brumer's proof of Leopoldt's conjecture for abelian fields (see also [1], [13]). Assume that $\text{rank}_{\mathbb{Z}_p} \mathcal{T}'_q < r$. Then there are elements a_1, \dots, a_r of \mathbb{Z}_p which satisfies

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in } \mathcal{U}_{P_h}^1$$

for all $h = 1, \dots, u$, and $a_d \neq 0$ with some d . Since $\beta_i = \alpha_i / \alpha_i^J$ and α_i is a conjugate of α_1 , we also see that

$$\prod_{\sigma \in \text{Gal}(k^D/\mathbb{Q})} (\alpha_1^{\sigma\tau^{-1}})^{x(\sigma)} = 1 \quad \text{in } \mathcal{U}_{P_1}^1$$

for all $\tau \in \text{Gal}(k^D/\mathbb{Q})$, where $x(\sigma) \in \mathbb{Z}_p$ satisfying $x(\sigma) \neq 0$ with some σ . Fix an embedding $k_{P_1}^D \rightarrow \mathbb{C}_p$. By taking the (normalized) p -adic logarithm of the above equation, we see

$$\sum_{\sigma \in \text{Gal}(k^D/\mathbb{Q})} x(\sigma) \log_p \alpha_1^{\sigma\tau^{-1}} = 0.$$

This implies that the determinant of the matrix $(\log_p \alpha_1^{\sigma\tau^{-1}})_{\sigma, \tau}$ is 0.

On the other hand, $\alpha_1, \dots, \alpha_r, \alpha_1^J, \dots, \alpha_r^J$ are multiplicative independent in $(k^D)^\times$. Then we can see that $\log_p \alpha_1, \dots, \log_p \alpha_r, \log_p \alpha_1^J, \dots, \log_p \alpha_r^J$ are linearly independent over \mathbb{Q} . By Baker-Brumer's theorem (see Brumer [1], Washington [13]), they are also linearly independent over $\overline{\mathbb{Q}}$ in \mathbb{C}_p . Hence the determinant of the matrix $(\log_p \alpha_1^{\sigma\tau^{-1}})_{\sigma, \tau}$ is *not* 0. It is a contradiction. Then we conclude that

$$\text{rank}_{\mathbb{Z}_p} \mathcal{T}'_q = \text{rank}_{\mathbb{Z}_p} \mathcal{T}_q = \text{rank}_{\mathbb{Z}_p} \mathcal{I}_p = r.$$

Next, we shall consider the case S. Assume that p splits in K/k . That is, $s = t$ and the number of primes of K lying above p is $2t$. The outline of the proof is the same as the case NS. Let \mathcal{T} be the closure of the diagonal image of T in $\prod_{j=1}^t \widehat{K_{\mathfrak{P}_j}^\times} \times \prod_{j=1}^t \widehat{K_{\mathfrak{P}_j^J}^\times}$. In this case, we shall show $\text{rank}_{\mathbb{Z}_p} T = r + t$.

Assume that $\text{rank}_{\mathbb{Z}_p} T < r + t$. Then there are elements a_1, \dots, a_{r+t} of \mathbb{Z}_p which satisfies

$$\begin{aligned} \beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} \rho_1^{a_{r+1}} \rho_2^{a_{r+2}} \cdots \rho_t^{a_{r+t}} &= 1 \quad \text{in } \mathcal{U}_{\mathfrak{P}_j}^1, \quad \text{and} \\ \beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} \rho_1^{a_{r+1}} \rho_2^{a_{r+2}} \cdots \rho_t^{a_{r+t}} &= 1 \quad \text{in } \mathcal{U}_{\mathfrak{P}_j^J}^1 \end{aligned}$$

for all $1 \leq j \leq t$. However, $v_{\mathfrak{P}_j}(\rho_j) \neq 0$ (for $1 \leq j \leq t$) by the definition of ρ_j . The above equality implies that a_{r+j} must be 0 for $1 \leq j \leq t$. Hence we obtain the equalities

$$\begin{aligned} \beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} &= 1 \quad \text{in } \mathcal{U}_{\mathfrak{P}_j}^1, \quad \text{and} \\ \beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} &= 1 \quad \text{in } \mathcal{U}_{\mathfrak{P}_j^J}^1 \end{aligned}$$

for all $1 \leq j \leq t$. Recall that k^D is the decomposition field of K/\mathbb{Q} for q . We denote by P_1, \dots, P_u the primes of k^D lying above p . As noted before (in the proof for the case NS), we can show $\mathcal{U}_{P_h}^1 \rightarrow \prod_{\mathfrak{P}|P_h} \mathcal{U}_{\mathfrak{P}}^1$ is injective. Hence we see

$$\beta_1^{a_1} \beta_2^{a_2} \cdots \beta_r^{a_r} = 1 \quad \text{in } \mathcal{U}_{P_h}^1$$

for all $1 \leq h \leq u$, and $a_i \neq 0$ with some i . The rest of the proof is quite same as that of for the case NS. \square

Since N is an abelian extension of k_∞ , we can take a unique intermediate field N^+ of N/k_∞ which satisfies $\text{Gal}(N^+/k_\infty) \cong \mathbb{Z}_p^{\oplus r+s}$. Similarly, we also able to take a unique intermediate field N_q^+ of N_q/k_∞ satisfying $\text{Gal}(N_q^+/k_\infty) \cong \mathbb{Z}_p^{\oplus r}$. (Note that $N_q^+ \subseteq N^+$, and $N_q^+ = N^+$ for the case NS.) Then we obtain the following:

Proposition 3.4. *N^+/K_∞ is unramified outside $\{p, q\}$, and a subgroup of $\text{Gal}(N^+/k_\infty)$ generated by the inertia groups for the primes lying above q has finite index. $N_q^+ \cap M_p(k_\infty)/k_\infty$ is a finite extension.*

4. PROOF OF THEOREM 1.1

We will use the same notation and symbols defined in section 3. Our strategy of the Proof of Theorem 1.1 is similar to that of Theorem A. However, our situation has a difficulty which comes from the fact that $\text{Gal}(M_p(k_\infty)/k_\infty)$ can be non-trivial. Assume that K, k , and p satisfy (A) stated in section 2.

We shall recall and define the following symbols:

- $M_{p,q}(k_\infty)$: the maximal pro- p abelian extension of k_∞ unramified outside $\{p, q\}$,
- $M_p(k_\infty)$: the maximal pro- p abelian extension of k_∞ unramified outside p ,
- $M_q(k_\infty)$: the maximal pro- p abelian extension of k_∞ unramified outside q ,
- $L(k_\infty)$: the maximal unramified pro- p abelian extension of k_∞ ,
- $\mathfrak{X}_{p,q}(k_\infty) = \text{Gal}(M_{p,q}(k_\infty)/k_\infty)$,
- $\mathfrak{X}_p(k_\infty) = \text{Gal}(M_p(k_\infty)/k_\infty)$,
- $X_q(k_\infty) = \text{Gal}(M_q(k_\infty)/k_\infty)$,
- $X(k_\infty) = \text{Gal}(L(k_\infty)/k_\infty)$.

We also define the following notation:

- $\Gamma = \text{Gal}(K_\infty/K)$ (we often identify Γ with $\text{Gal}(k_\infty/k)$.),
- γ : fixed topological generator of Γ ,
- κ : (p -adic) cyclotomic character,
- $\Lambda = \mathbb{Z}_p[[T]] \cong \mathbb{Z}_p[[\Gamma]] : 1 + T \leftrightarrow \gamma$,
- $\dot{T} = \kappa(\gamma)(1 + T)^{-1} - 1 \in \Lambda$.

For a finitely generated torsion Λ -module A , we denote by $\text{char}_\Lambda A$ the characteristic ideal of A (see, e.g., [13]). For finitely generated torsion Λ -modules A and B , we write $A \sim B$ when they are pseudo-isomorphic. We denote by $X(K_\infty)^- := X(K_\infty)^{1-J}$ the minus part of $X(K_\infty)$.

We recall the fact that $\mathfrak{X}_p(k_\infty)$ relates to $X(K_\infty)^-$ by Kummer duality. Let $f(T) \in \Lambda$ be a generator of $\text{char}_\Lambda X(K_\infty)^-$. We note that $f(T)$ is not divisible by p because K is an abelian field (Ferrero-Washington's theorem). It is known that $f(\dot{T}) \in \Lambda$ generates

$\text{char}_\Lambda \mathfrak{X}_p(k_\infty)$. By the result of Greenberg [2], we know that the power of T dividing $f(T)$ is T^s , where $s = 0$ for the case NS, and $s = t$ for the case S. Hence the power of \dot{T} dividing $f(\dot{T})$ is just \dot{T}^s . For the case NS, we see that $f(\dot{T})$ is prime to \dot{T} .

For $i = 1, \dots, t$, let $k_{n,i}$ be the completion of k_n at the unique prime lying above \mathfrak{p}_i , and $\mathcal{U}^1(k_{n,i})$ the group of principal units in $k_{n,i}$. Let $\phi(E_{k_n})$ be the diagonal image of E_{k_n} in $\prod_i k_{n,i}^\times$, and \mathcal{E}_n the closure of $\phi(E_{k_n}) \cap \prod_i \mathcal{U}^1(k_{n,i})$. We put $\mathcal{U} = \varprojlim \prod_i \mathcal{U}^1(k_{n,i})$, and $\mathcal{E} = \varprojlim \mathcal{E}_n$, where the projective limits are taken with respect to the norm mappings. Recall the exact sequence:

$$0 \rightarrow \text{Gal}(M_p(k_\infty)/L(k_\infty)) \rightarrow \mathfrak{X}_p(k_\infty) \rightarrow X(k_\infty) \rightarrow 0,$$

and the fact that $\text{Gal}(M_p(k_\infty)/L(k_\infty)) \cong \mathcal{U}/\mathcal{E}$. We note that $\varprojlim \mathcal{U}^1(k_{n,i})$ contains $\varprojlim \mu_{p^n} \cong \Lambda/\dot{T}$ for the case S (see [12], etc.). Hence \mathcal{U} contains a submodule which is isomorphic to $(\Lambda/\dot{T})^{\oplus s}$, and \mathcal{E} does not contain this submodule because k is totally real. From the above facts, we obtain the following:

Lemma 4.1. *There is a pseudo-isomorphism of finitely generated torsion Λ -modules:*

$$\text{Gal}(M_p(k_\infty)/L(k_\infty)) \sim (\Lambda/\dot{T})^{\oplus s} \oplus E,$$

where E is an elementary torsion Λ -module (see Iwasawa [6], Washington [13]) whose characteristic ideal is prime to (\dot{T}) . Moreover, the characteristic ideal of $X(k_\infty)$ is prime to (\dot{T}) .

Let N^+ and N_q^+ be extensions over k_∞ defined in section 3 (see the paragraph before Lemma 3.4).

Lemma 4.2. (see also Greenberg [3]) $M_{p,q}(k_\infty) = M_p(k_\infty)N_q^+$.

Proof. Though this fact is already shown in [3], we will give a detailed proof for a convenient to the reader. Let $\widetilde{M}_{p,q}(k_\infty)$ be the maximal pro- p extension of k_∞ unramified outside $\{p, q\}$. By Theorem 3 of Iwasawa [7] and Ferrero-Washington's theorem, we see that $\text{Gal}(\widetilde{M}_{p,q}(k_\infty)/k_\infty)$ is a free pro- p group whose minimal number of generators is $\lambda^- + r$, where $\lambda^- = \text{rank}_{\mathbb{Z}_p} X(K_\infty)^-$. (Note that every prime lying above q actually ramifies in $\widetilde{M}_{p,q}(k_\infty)/k_\infty$ by Lemma 3.2.) By taking the abelian quotient of $\text{Gal}(\widetilde{M}_{p,q}(k_\infty)/k_\infty)$, we see that $\mathfrak{X}_{p,q}(k_\infty) \cong \mathbb{Z}_p^{\oplus \lambda^- + r}$ as a \mathbb{Z}_p -module.

On the other hand, we can see that $M_p(k_\infty) \cap N_q^+/k_\infty$ is a finite extension by using Lemma 3.2 (2). Hence

$$\text{rank}_{\mathbb{Z}_p} \text{Gal}(M_p(k_\infty)N_q^+/k_\infty) = \text{rank}_{\mathbb{Z}_p} \mathfrak{X}_p(k_\infty) + r = \lambda^- + r.$$

Since N_q^+/k_∞ is unramified outside $\{p, q\}$, we see $M_{p,q}(k_\infty) \supseteq M_p(k_\infty)N_q^+$. Then we have a surjection of finitely generated \mathbb{Z}_p -modules $\mathfrak{X}_{p,q}(k_\infty) \rightarrow \text{Gal}(M_p(k_\infty)N_q^+/k_\infty)$ whose

kernel is finite. However $\mathfrak{X}_{p,q}(k_\infty)$ has no \mathbb{Z}_p -torsion element, and hence we conclude that $M_{p,q}(k_\infty) = M_p(k_\infty)N_q^+$. \square

For a finitely generated torsion Λ -module A , we can define the “multiplication by \dot{T} endomorphism” of A , and we denote by $A[\dot{T}]$ (reps. A/\dot{T}) its kernel (resp. cokernel):

$$0 \rightarrow A[\dot{T}] \rightarrow A \xrightarrow{\dot{T}} A \rightarrow A/\dot{T} \rightarrow 0.$$

Note that Γ acts on $\text{Gal}(M_{p,q}(k_\infty)/L(k_\infty))$ and then it is also a finitely generated torsion Λ -module. Let M' be the intermediate field of $M_{p,q}(k_\infty)/L(k_\infty)$ corresponding to $\dot{T}\text{Gal}(M_{p,q}(k_\infty)/L(k_\infty))$. Hence $\text{Gal}(M'/L(k_\infty))$ is isomorphic to $\text{Gal}(M_{p,q}(k_\infty)/L(k_\infty))/\dot{T}$.

Lemma 4.3. $M_q(k_\infty)$ is contained in M' .

Proof. By class field theory, $\text{Gal}(M_q(k_\infty)/L(k_\infty))$ is isomorphic to a quotient of $\varprojlim (\widehat{O_{k_n}/q})^\times$. As a Λ -module, $\varprojlim (\widehat{O_{k_n}/q})^\times$ is isomorphic to $(\Lambda/\dot{T})^{\oplus r}$. Hence \dot{T} annihilates $\text{Gal}(M_q(k_\infty)/L(k_\infty))$, and then $\text{Gal}(M_q(k_\infty)/L(k_\infty))/\dot{T} = \text{Gal}(M_q(k_\infty)/L(k_\infty))$. From the restriction map

$$\text{Gal}(M_{p,q}(k_\infty)/L(k_\infty)) \rightarrow \text{Gal}(M_q(k_\infty)/L(k_\infty)) \rightarrow 0,$$

we obtain a surjection

$$\text{Gal}(M_{p,q}(k_\infty)/L(k_\infty))/\dot{T} \rightarrow \text{Gal}(M_q(k_\infty)/L(k_\infty)) \rightarrow 0.$$

By the definition of M' , we see $M_q(k_\infty) \subseteq M'$. \square

Lemma 4.4. $L(k_\infty)N^+$ is contained in M' .

Proof. Note that $\text{Gal}(L(k_\infty)N^+/L(k_\infty)) \cong \text{Gal}(N^+/N^+ \cap L(k_\infty))$, and $\text{Gal}(N^+/N^+ \cap L(k_\infty))$ is a subgroup of $\text{Gal}(N^+/k_\infty)$. By the construction of N^+ , we see that \dot{T} annihilates $\text{Gal}(N^+/k_\infty)$, and hence also annihilates $\text{Gal}(L(k_\infty)N^+/L(k_\infty))$. The rest of the proof is similar to that of Lemma 4.3. \square

Lemma 4.5. $M'/L(k_\infty)N^+$ is a finite extension.

Proof. We shall show that $\text{rank}_{\mathbb{Z}_p} \text{Gal}(M'/L(k_\infty)) = \text{rank}_{\mathbb{Z}_p} \text{Gal}(L(k_\infty)N^+/L(k_\infty))$. By Proposition 3.3, we see that $N \cap L(k_\infty)/k_\infty$ is a finite extension. Hence $\text{rank}_{\mathbb{Z}_p} \text{Gal}(L(k_\infty)N^+/L(k_\infty))$ is equal to $\text{rank}_{\mathbb{Z}_p} \text{Gal}(N^+/k_\infty) = r + s$.

On the other hand, $M_{p,q}(k_\infty) = M_p(k_\infty)N_q^+$ by Lemma 4.2, and $M_p(k_\infty) \cap N_q^+/k_\infty$ is a finite extension by Lemma 3.2. By using Lemma 4.1, we can obtain the following pseudo-isomorphisms:

$$\mathfrak{X}_{p,q}(k_\infty) \sim \mathfrak{X}_p(k_\infty) \oplus \text{Gal}(N_q^+/k_\infty) \sim (\Lambda/\dot{T})^{\oplus r+s} \oplus E',$$

where E' is an elementary torsion Λ -module whose characteristic ideal is prime to (\dot{T}) . Hence, $\text{rank}_{\mathbb{Z}_p} \mathfrak{X}_{p,q}(k_\infty)/\dot{T} = r + s$.

The following exact sequence:

$$0 \rightarrow \text{Gal}(M_{p,q}(k_\infty)/L(k_\infty)) \rightarrow \mathfrak{X}_{p,q}(k_\infty) \rightarrow X(k_\infty) \rightarrow 0$$

induces the exact sequence:

$$X(k_\infty)[\dot{T}] \rightarrow \text{Gal}(M_{p,q}(k_\infty)/L(k_\infty))/\dot{T} \rightarrow \mathfrak{X}_{p,q}(k_\infty)/\dot{T} \rightarrow X(k_\infty)/\dot{T} \rightarrow 0.$$

Since $\text{char}_\Lambda X(k_\infty)$ is prime to (\dot{T}) , both of $X(k_\infty)[\dot{T}]$ and $X(k_\infty)/\dot{T}$ are finite by Lemma 4.1. Hence $\text{rank}_{\mathbb{Z}_p} \text{Gal}(L(k_\infty)N^+/L(k_\infty))$ is equal to $\text{rank}_{\mathbb{Z}_p} \mathfrak{X}_{p,q}(k_\infty)/\dot{T} = \text{rank}_{\mathbb{Z}_p} \text{Gal}(M'/L(k_\infty))$. \square

For a Galois group G appeared below, we denote $\mathcal{I}(G)$ by the subgroup of G generated by the inertia groups for all primes lying above p .

Lemma 4.6. $\text{rank}_{\mathbb{Z}_p} \mathcal{I}(\text{Gal}(N^+L(k_\infty)/L(k_\infty))) = r + s$.

Proof. We shall take a prime \mathcal{P} of k_∞ lying above p . Let $I_{\mathcal{P}}$ be the inertia subgroup of $\text{Gal}(N^+/k_\infty)$ for \mathcal{P} . Similarly, let $I'_{\mathcal{P}}$ be the inertia subgroup of $\text{Gal}(N^+L(k_\infty)/k_\infty)$ for \mathcal{P} . Then the restriction map induces a surjection $I'_{\mathcal{P}} \rightarrow I_{\mathcal{P}}$. Hence there is a surjection $\mathcal{I}(\text{Gal}(N^+L(k_\infty)/k_\infty)) \rightarrow \mathcal{I}(\text{Gal}(N^+/k_\infty))$. By Proposition 3.3, $\text{rank}_{\mathbb{Z}_p} \mathcal{I}(\text{Gal}(N^+/k_\infty)) = r + s$. We see that $\text{rank}_{\mathbb{Z}_p} \mathcal{I}(\text{Gal}(N^+L(k_\infty)/k_\infty)) \geq r + s$. Since $L(k_\infty)/k_\infty$ is an unramified extension, $\mathcal{I}(\text{Gal}(N^+L(k_\infty)/k_\infty))$ is contained in $\text{Gal}(N^+L(k_\infty)/L(k_\infty))$. By these results, we see that $\text{rank}_{\mathbb{Z}_p} \mathcal{I}(\text{Gal}(N^+L(k_\infty)/L(k_\infty))) = r + s$. \square

We shall finish to prove Theorem 1.1. By Lemma 4.6, $\text{rank}_{\mathbb{Z}_p} \mathcal{I}(\text{Gal}(N^+L(k_\infty)/L(k_\infty))) = r + s$. Moreover, $\text{rank}_{\mathbb{Z}_p} \mathcal{I}(\text{Gal}(M'/L(k_\infty)))$ is also $r + s$ because $M'/N^+L(k_\infty)$ is a finite extension (Lemma 4.5). From the proof of Lemma 4.5, we see that $\text{rank}_{\mathbb{Z}_p} \text{Gal}(M'/L(k_\infty))$ is $r + s$. Then $\mathcal{I}(\text{Gal}(M'/L(k_\infty)))$ is a finite index subgroup of $\text{Gal}(M'/L(k_\infty))$. By Lemma 4.3, $M_q(k_\infty)$ is an intermediate field of $M'/L(k_\infty)$. Since $M_q(k_\infty)/L(k_\infty)$ is unramified at all primes lying above p , we can see that $M_q(k_\infty)$ is contained in the fixed field of $\mathcal{I}(\text{Gal}(M'/L(k_\infty)))$. This implies that $M_q(k_\infty)/L(k_\infty)$ is a finite extension.

We have shown Theorem 1.1 for k and p satisfying (A). Then, as noted in section 2, we obtain Theorem 1.1 for general k and p . \square

5. SLIGHT GENERALIZATION OF THEOREM 1.1

In this section, we shall give a simple remark that the inverse of Lemma 2.1 holds under a (strict) condition.

Lemma 5.1. *Let k'/k be a finite extension of algebraic number fields. Assume that every prime in k_∞ lying above q does not split in k'_∞ . If $\text{Gal}(M_q(k_\infty)/L(k_\infty))$ is finite, then $\text{Gal}(M_q(k'_\infty)/L(k'_\infty))$ is also finite.*

Proof. Let

$$I_n : (\widehat{O_{k'_n}/q})^\times \rightarrow (\widehat{O_{k_n}/q})^\times$$

be the homomorphism induced from the natural embedding. We claim that the order of the cokernel $\text{Coker}(I_n)$ is bounded as $n \rightarrow \infty$. Assume that n is sufficiently large such that every prime of k_n lying above q does not split in k'_∞ . We also may assume that $k'_n \cap k_\infty = k_n$. Let \mathfrak{q} be a prime of k_n lying above q , and \mathfrak{Q} the unique prime of k'_n lying above \mathfrak{q} . To see the claim, it is sufficient to show that the order of the cokernel of the homomorphism

$$(\widehat{O_{k_n}/\mathfrak{q}})^\times \rightarrow (\widehat{O_{k'_n}/\mathfrak{Q}})^\times$$

(induced from the natural mapping) is bounded as $n \rightarrow \infty$. However, this fact easily follows because the above map is injective. We have shown the claim.

Then the order of the cokernel $\text{Gal}(M_q(k_n)/L(k_n)) \rightarrow \text{Gal}(M_q(k'_n)/L(k'_n))$ induced from I_n is bounded as $n \rightarrow \infty$. By using a similar argument given in the proof of Lemma 2.1, we can see that if the order of $\text{Gal}(M_q(k_n)/L(k_n))$ is bounded, then order of $\text{Gal}(M_q(k'_n)/L(k'_n))$ is also bounded. \square

The above lemma implies that Theorem 1.1 can be generalized for some non-abelian fields.

6. \mathbb{Z}_p -RANK OF S -RAMIFIED IWASAWA MODULES

We shall lead a formula of the \mathbb{Z}_p -rank of S -ramified Iwasawa modules (for general S) from Theorem 1.1. As same as Theorem 1.1, the strategy of our proof is quite similar to that of given in [5].

In this section, we will use the following notation (similar to Greither's [4] or Tsuji's [12] but slightly different):

- p : fixed odd prime,
- S : finite set of *rational* primes not including p ,
- F : finite abelian extension of \mathbb{Q} unramified at p ,
- $K = F(\mu_p)$,
- $K_n = K(\mu_{p^{n+1}})$,
- $K_\infty = \cup_{n \geq 1} K_n$: the cyclotomic \mathbb{Z}_p -extension of K ,
- $G = \text{Gal}(K_\infty/\mathbb{Q}_\infty) \cong \text{Gal}(K/\mathbb{Q})$,
- $\Gamma = \text{Gal}(K_\infty/K)$,
- G_p : Sylow p -subgroup of G ,
- G_0 : non- p -part of G (the maximal subgroup of G consists of the elements having prime to p order),
- γ : fixed topological generator of Γ ,
- κ : (p -adic) cyclotomic character,
- ω : (p -adic) Teichmüller character,

- $J \in G$: complex conjugation.

Let χ be a p -adic character of G . We denote by $\mathbb{Q}_p(\chi)$ the extension of \mathbb{Q}_p by adjoining the values of χ , and O_χ the valuation ring of $\mathbb{Q}_p(\chi)$. We put $d_\chi = [\mathbb{Q}_p(\chi) : \mathbb{Q}_p]$. Let \underline{O}_χ be a free rank one O_χ -module such that $\sigma \in G$ acts as $\chi(\sigma)$. For a $\mathbb{Z}_p[G]$ -module M , we put $M_\chi = M \otimes_{\mathbb{Z}_p[G]} \underline{O}_\chi$, which is called the “ χ -quotient” in [12] (or the “ χ -part” in [4]). The functor taking the χ -quotient is right exact. We also put

$$e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \text{tr}_{\mathbb{Q}_p(\chi)/\mathbb{Q}_p}(\chi(\sigma)) \sigma^{-1} \in \mathbb{Q}_p[G].$$

If p does not divide $|G|$, then $M_\chi \cong e_\chi M$. In general, we see

$$M_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong (M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_\chi \cong e_\chi (M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

For more informations about the χ -quotient, see [4], [12] for example.

We also give some simple remarks. For a $\mathbb{Z}_p[G]$ -module M , we put $M^\pm = M^{1 \pm J}$. Since p is odd, we have a decomposition $M \cong M^+ \oplus M^-$. For a character χ of G , we see that

$$\begin{aligned} M_\chi &\cong (M^+ \oplus M^-)_\chi \\ &= (M^+ \oplus M^-) \otimes_{\mathbb{Z}_p[G]} \underline{O}_\chi \\ &\cong (M^+ \otimes_{\mathbb{Z}_p[G]} \underline{O}_\chi) \oplus (M^- \otimes_{\mathbb{Z}_p[G]} \underline{O}_\chi) \\ &= M_\chi^+ \oplus M_\chi^-. \end{aligned}$$

We claim that if χ is odd, then M_χ^+ is trivial. Let

$$(a \otimes b) \in M^+ \otimes_{\mathbb{Z}_p[G]} \underline{O}_\chi = M_\chi^+.$$

Note that J acts trivially on M^+ and acts as -1 on \underline{O}_χ . Hence the equality

$$(a \otimes b) = (Ja \otimes b) = (a \otimes Jb) = (a \otimes -b)$$

implies that $(a \otimes 2b) = 2(a \otimes b) = 0$. Since p is odd, we obtain the claim. Similarly, we can see that if χ is even, then M_χ^- is trivial.

For a rational prime q distinct from p , we put

$$R_q = \varprojlim (\widehat{O_{K_n}/q})^\times$$

Let r be the number of primes of K_∞ lying above q . Then $\text{rank}_{\mathbb{Z}_p} R_q = r$. Since q is a rational prime, G acts on R_q . We shall determine the \mathbb{Z}_p -rank of $(R_q)_\chi$.

First, we assume that q is unramified in K (i.e., the conductor of F is prime to q). Let D be the decomposition group of $\text{Gal}(K_\infty/\mathbb{Q})$ for q . Then we can write $D \cong D_p \times D_0$, where $D_p \cong \mathbb{Z}_p$ and D_0 is a finite cyclic group whose order is prime to p . We may regard D_0 as a subgroup of G_0 . Note that $\text{Gal}(K_\infty/\mathbb{Q})$ is isomorphic to $\Gamma \times G_p \times G_0$. Then we can take a generator of D_p of the form $\gamma^{p^m} \sigma_p$ with some $m \geq 0$ and $\sigma_p \in G_p$. We also take a generator $\sigma_0 \in G_0$ of D_0 . Hence D is a procyclic group generated by $\gamma^{p^N} \sigma_p \sigma_0$.

In the above choice of the generator of D_p , we can see that m and σ_p is uniquely determined. (Since $D_p \cong \mathbb{Z}_p$, every generator of D_p is written by the form $(\gamma^{p^m} \sigma_p)^\alpha$ with $\alpha \in \mathbb{Z}_p^\times$.)

Lemma 6.1. R_q is a cyclic $\mathbb{Z}_p[G][[\Gamma]]$ -module.

Proof. Fix a sufficiently large integer n_0 such that every prime in K_{n_0} lying above q remains prime in K_m for all $m \geq n_0$. Let n be an integer which satisfies $n \geq n_0$. We put $G^{(n)} = \text{Gal}(K_n/\mathbb{Q})$. Let \mathfrak{q} be a primes of q in K_n . We remark that $\mu_{p^{n+1}} \subset K_n$ and $\mu_{p^{n+2}} \not\subset K_n$. Under the assumption on n , we can see that the Sylow p -subgroup of $(O_{K_n}/\mathfrak{q})^\times$ is generated by $\zeta_{p^{n+1}} \pmod{\mathfrak{q}}$ with a generator $\zeta_{p^{n+1}}$ of $\mu_{p^{n+1}}$. Let $\{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\}$ be the set of primes of K_n lying above q . We assumed that q is unramified in K_∞/\mathbb{Q} , then $qO_{K_n} = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r$. Since the action of $G^{(n)}$ on $\{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\}$ is transitive, we can see that the Sylow p -subgroup of $(O_{K_n}/q)^\times$ is isomorphic to $\mu_{p^{n+1}}[G^{(n)}/D^{(n)}]$ as a $\mathbb{Z}_p[G^{(n)}]$ -module, where $D^{(n)}$ is the decomposition subgroup of $G^{(n)}$ for q . Take an element α_n of O_{K_n} which satisfies

$$\alpha_n \equiv \zeta_{p^{n+1}} \pmod{\mathfrak{q}_1}, \quad \alpha_n \equiv 1 \pmod{\mathfrak{q}_2}, \quad \dots, \quad \alpha_n \equiv 1 \pmod{\mathfrak{q}_r}.$$

Then $\alpha_n \pmod{q}$ is a generator of the Sylow p -subgroup of $(O_{K_n}/q)^\times$ as a $\mathbb{Z}_p[G^{(n)}]$ -module. Hence the Sylow p -subgroup of $(O_{K_n}/q)^\times$ (which is isomorphic to $(\widehat{O_{K_n}/q})^\times$) is a cyclic $\mathbb{Z}_p[G^{(n)}]$ -module.

We can choose a suitable set of generators $\{\alpha_n\}$ such that $N_{K_m/K_n}(\alpha_m) \equiv \alpha_n \pmod{q}$ for all $m > n \geq n_0$. Hence we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccc} \mathbb{Z}_p[G^{(m)}] & \rightarrow & (\widehat{O_{K_m}/q})^\times & \rightarrow & 0 \\ \downarrow & & \downarrow & & \\ \mathbb{Z}_p[G^{(n)}] & \rightarrow & (\widehat{O_{K_n}/q})^\times & \rightarrow & 0, \end{array}$$

where the left vertical mapping is induced from the restriction mapping, and the right vertical mapping is induced from the norm mapping. Since $\varprojlim \mathbb{Z}_p[G^{(n)}] \cong \mathbb{Z}_p[G][[\Gamma]]$, we obtain the assertion. \square

Hence there is a surjection $\varphi : \mathbb{Z}_p[G][[\Gamma]] \rightarrow R_q$. We note that $\gamma^{p^m} \sigma_p \sigma_0$ acts on R_q as $\kappa(\gamma^{p^m} \sigma_p \sigma_0)$. (Recall that κ is the cyclotomic character.) Then the kernel of φ contains an ideal generated by $\gamma^{p^m} \sigma_p \sigma_0 - \kappa(\gamma^{p^m} \sigma_p \sigma_0)$.

By taking the χ -quotient, we obtain a surjection $\varphi_\chi : O_\chi[[\Gamma]] \rightarrow (R_q)_\chi$, and the kernel of φ_χ contains $\chi(\sigma_p \sigma_0) \gamma^{p^m} - \kappa(\gamma^{p^m} \sigma_p \sigma_0)$. We may regard $(R_q)_\chi$ as a $O_\chi[[T]]$ -module via the isomorphism $O_\chi[[\Gamma]] \cong O_\chi[[T]]$ with $\gamma \mapsto 1 + T$. We put $\Lambda_\chi = O_\chi[[T]]$, and $\kappa_0 = \kappa(\gamma) \in 1 + p\mathbb{Z}_p$. Then we see that $(R_q)_\chi$ is annihilated by

$$f_{q,\chi}(T) = (1 + T)^{p^m} - \chi^{-1}(\sigma_p \sigma_0) \kappa(\sigma_p \sigma_0) \kappa_0^{p^m} \in \Lambda_\chi.$$

Let \mathfrak{P} be the maximal ideal of O_χ . Since $\kappa_0 \in 1 + p\mathbb{Z}_p$, if

$$\chi^{-1}(\sigma_p \sigma_0) \kappa(\sigma_p \sigma_0) \not\equiv 1 \pmod{\mathfrak{P}},$$

then $f_{q,\chi}(T)$ is a unit polynomial, and hence $(R_q)_\chi$ is trivial. We see

$$\chi^{-1}(\sigma_p \sigma_0) \kappa(\sigma_p \sigma_0) = \chi^{-1} \kappa(\sigma_0) \chi^{-1} \kappa(\sigma_p) = \chi^{-1} \omega(\sigma_0) \chi^{-1} \kappa(\sigma_p).$$

Note that $\chi^{-1} \kappa(\sigma_p)$ is a p -power root of unity and then congruent to 1 modulo \mathfrak{P} . Moreover, $\chi^{-1} \omega(\sigma_0)$ is a root of unity whose order is prime to p . Then $\chi^{-1} \omega(\sigma_0) \equiv 1 \pmod{\mathfrak{P}}$ if and only if $\chi^{-1} \omega(\sigma_0) = 1$. Consequently, we showed that if $\chi^{-1} \omega(\sigma_0) \neq 1$, then $(R_q)_\chi$ is trivial.

We can see that the number of characters χ satisfying $\chi^{-1} \omega(\sigma_0) = 1$ is just $|G/D_0|$. (It is equal to the number of characters χ' of G satisfying $\chi'(D_0) = 1$.) Though $(R_q)_\chi$ is non-trivial, it is annihilated by $f_{q,\chi}(T)$, and then $\text{rank}_{\mathbb{Z}_p}(R_q)_\chi \leq d_\chi p^m$. By considering these facts, we obtain the inequality:

$$r = \text{rank}_{\mathbb{Z}_p} R_q = \sum_{\chi} \text{rank}_{\mathbb{Z}_p}(R_q)_\chi \leq \sum_{\chi} d_\chi p^m = |G/D_0| \times p^m,$$

where χ runs all representatives of the conjugacy classes satisfying $\chi^{-1} \omega(\sigma_0) = 1$ in the above sums. (We also give some remarks. The second equation follows from the fact that $R_q \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{\chi} (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Moreover, $\sum_{\chi} d_\chi = |G/D_0|$, and m is independent of χ).

We claim that $r = |G/D_0| \times p^m$. Let K^D be the decomposition field of K_∞/\mathbb{Q} for q . Then the p -part of $[K^D : \mathbb{Q}]$ is equal to the p -part of $[K_m : \mathbb{Q}]$. Hence this is equal to $|G_p| \times p^m$. On the other hand, the non- p -part of $[K^D : \mathbb{Q}]$ is equal to $|G_0/D_0|$. We see

$$[K^D : \mathbb{Q}] = |G_p| \times p^m \times |G_0/D_0| = |G/D_0| \times p^m.$$

Since $r = [K^D : \mathbb{Q}]$, the claim follows.

From this claim, we see that the above inequality is just an equality. Hence for all character χ satisfying $\chi^{-1} \omega(\sigma_0) = 1$, the \mathbb{Z}_p -rank of $(R_q)_\chi$ is $d_\chi p^m$. We also note that $\kappa(\sigma_p) = 1$ because σ_p fixes all elements of μ_{p^n} for all n . Hence, when $\chi^{-1} \omega(\sigma_0) = 1$, we can write

$$f_{q,\chi}(T) = (1 + T)^{p^m} - \chi^{-1}(\sigma_p) \kappa_0^{p^m}.$$

Secondly, we allow the case that q is ramified in K . Let I be the inertia subgroup of $\text{Gal}(K/\mathbb{Q})$ for q , and K^I the inertia field of K/\mathbb{Q} for q . We remark that all primes lying above q are totally ramified in K_n/K_n^I . Hence $(\widehat{O_{K_n}/q})^\times \cong (\widehat{O_{K_n^I}/q})^\times$ for all n . We put

$$R_q^I = \varprojlim (\widehat{O_{K_n^I}/q})^\times$$

Let χ be a character of G . If $\chi(I) = 1$, then χ is also a character of $\text{Gal}(K^I/\mathbb{Q})$, and hence $(R_q)_\chi \cong (R_q^I)_\chi$. From this, if $\chi(I) \neq 1$, we see that $(R_q)_\chi$ is finite by comparing \mathbb{Z}_p -ranks of each modules.

Since q is unramified in $\mathbb{Q}(\mu_{p^\infty})$ (where $\mu_{p^\infty} = \bigcup_{n \geq 1} \mu_{p^n}$), we see that K_∞^I contains μ_{p^∞} . Then the proof of Lemma 6.1 also works for K_∞^I .

We also determine the structure of $(R_q)_\chi$ in general case. Assume that $\chi(I) = 1$. Then $\chi(\sigma)$ for $\sigma \in \text{Gal}(K^I/\mathbb{Q}) \cong G/I$ is well defined. Repeating the argument given in the unramified case for K^I , we can take σ_0 and σ_p for q . (They are determined modulo I , and $\sigma_p \pmod{I}$ is uniquely determined. Hence $\chi(\sigma_p)$ is dependent only on q .) We also assume that $\chi^{-1}\omega(\sigma_0) = 1$. Since $\mathbb{Z}_p[G/I]_\chi \cong O_\chi$, we can take

$$f_{q,\chi}(T) = (1+T)^{p^m} - \chi^{-1}(\sigma_p)\kappa_0^{p^m}$$

as an element of $\Lambda_\chi = O_\chi[[T]]$. We see that $(R_q)_\chi$ is annihilated by $f_{q,\chi}(T)$ because $(R_q)_\chi \cong (R_q^I)_\chi$.

As a consequence, we obtained the following:

Proposition 6.2. *Let χ be a character of G . Then $(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-trivial if and only if χ satisfies $\chi(I) = 1$ and $\chi^{-1}\omega(\sigma_0) = 1$. Moreover, if $(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-trivial, then*

$$(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \Lambda_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

and $\text{rank}_{\mathbb{Z}_p}(R_q)_\chi = d_\chi p^m$.

By class field theory, we have the following exact sequence:

$$E_\infty \rightarrow R_q \rightarrow \text{Gal}(M_q(K_\infty)/L(K_\infty)) \rightarrow 0,$$

where $E_\infty = \varprojlim \widehat{E_{K_n}}$. Assume that χ is a non-trivial *even* character of G satisfying $\chi(I) = 1$ and $\chi^{-1}\omega(\sigma_0) = 1$. By taking the χ -quotient (it is right exact), we see

$$(E_\infty)_\chi \rightarrow (R_q)_\chi \rightarrow \text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \rightarrow 0$$

is exact. Since $(R_q)_\chi$ is annihilated by $f_{q,\chi}(T)$, we obtain the exact sequence:

$$(E_\infty)_\chi / f_{q,\chi}(T) \rightarrow (R_q)_\chi \rightarrow \text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \rightarrow 0.$$

By tensoring \mathbb{Q}_p , we also obtain the exact sequence:

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow \text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow 0.$$

Proposition 6.3. *For every non-trivial even character χ of G satisfying $\chi(I) = 1$ and $\chi^{-1}\omega(\sigma_0) = 1$, the mapping*

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

appeared above is an isomorphism as \mathbb{Q}_p -vector spaces.

Proof. As we noted before, we have a decomposition

$$\text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \cong \text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi^+ \oplus \text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi^-.$$

Moreover, we already know that $\text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi^-$ is trivial for every even character χ . Let K^+ be the maximal real subfield of K . Since p is odd, we see that $\text{Gal}(M_q(K_\infty)/L(K_\infty))^+$ is isomorphic to $\text{Gal}(M_q(K_\infty^+)/L(K_\infty^+))$. Hence we obtain

$$\text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \cong \text{Gal}(M_q(K_\infty^+)/L(K_\infty^+))_\chi$$

for every χ satisfying the assumption. (We note that χ can be viewed as a character of $\text{Gal}(K_\infty^+/\mathbb{Q}_\infty)$.)

By Theorem 1.1, we see that $\text{Gal}(M_q(K_\infty^+)/L(K_\infty^+))$ is finite, and hence we see that $\text{Gal}(M_q(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is trivial. From this, we have a surjection

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

By Proposition 6.2, $\dim_{\mathbb{Q}_p}(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = d_\chi p^m$. We shall calculate the dimension of $(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Let \mathcal{U} be the projective limit of semi local units in K_∞/K for the primes lying above p , \mathcal{E} the closure of the diagonal image of global units (see section 4). Since Leopoldt's conjecture is valid for all K_n , we see that \mathcal{E} is isomorphic to E_∞ . It is known that $\mathcal{E}_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a free cyclic $\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ -module. (See [4], [12]. Indeed, the Coleman homomorphism induces an injection from $\mathcal{E}_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ to a free cyclic $\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ -module, even when p splits in K/K^+ . Since $\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a PID, the assertion follows.) Then we see

$$\begin{aligned} (\mathcal{E}_\chi / f_{q,\chi}(T)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p &\cong (\mathcal{E}_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) / (f_{q,\chi}(T) \otimes 1) \\ &\cong (\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) / (f_{q,\chi}(T) \otimes 1) \\ &\cong (\Lambda_\chi / f_{q,\chi}(T)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. \end{aligned}$$

Hence we showed that $\dim_{\mathbb{Q}_p}(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = d_\chi p^m$. This implies the assertion. \square

Here we shall state our main result. Let χ be an arbitrary character of G . Let S be a finite set of rational primes which does not include p . In this case, G acts on $X_S(K_\infty)$ and hence its χ -quotient can be considered. We shall give a formula of $\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi$. For a prime $q \in S$, let I_q be the inertia subgroup of G for q . We also write $\sigma_{p,q}, \sigma_{0,q}, m_q$ as σ_p, σ_0, m for q (defined before), respectively. (Recall that $\sigma_{p,q}$ and $\sigma_{0,q}$ are determined modulo I_q .)

Theorem 6.4. *We put*

$$S_\chi = \{q \in S \mid \chi(I_q) = 1, \chi^{-1}\omega(\sigma_{0,q}) = 1\},$$

$$f_{q,\chi}(T) = (1+T)^{p^{m_q}} - \chi^{-1}(\sigma_{p,q})\kappa(\gamma)^{p^{m_q}} \in O_\chi[[T]],$$

and $F(T) = \text{lcm}_{q \in S_\chi} f_{q,\chi}(T)$. If S_χ is not empty, then

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} d_\chi p^{m_q} - P_\chi,$$

where

$$P_\chi = \begin{cases} 1 & (\chi = \omega) \\ 0 & (\chi : \text{odd}, \chi \neq \omega) \\ d_\chi \deg F(T) & (\chi : \text{even}). \end{cases}$$

If S_χ is empty, then $\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$.

Proof. Recall the following exact sequence:

$$E_\infty \rightarrow \bigoplus_{q \in S} R_q \rightarrow \text{Gal}(M_S(K_\infty)/L(K_\infty)) \rightarrow 0$$

which is stated in section 2. By Proposition 6.2, we see that $(R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is non-trivial if and only if $q \in S_\chi$. Hence, if S_χ is empty, then $\text{Gal}(M_S(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is trivial, and $\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$. In the following, we assume that S_χ is not empty. By taking the χ -quotient and tensoring \mathbb{Q}_p , we have the exact sequence:

$$(E_\infty)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\eta_\chi} \bigoplus_{q \in S_\chi} (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow \text{Gal}(M_S(K_\infty)/L(K_\infty))_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow 0.$$

It is sufficient to determine the cokernel of η_χ .

Since p is odd, we have a decomposition $E_\infty \cong E_\infty^+ \oplus E_\infty^-$, and we can see $E_\infty^- \cong \varprojlim \mu_{p^n}$. We also note that $(E_\infty)_\chi \cong (E_\infty^+)_\chi \oplus (E_\infty^-)_\chi$ for a character χ of G . It was already shown that if χ is an odd character, then $(E_\infty^+)_\chi$ is trivial, and hence $(E_\infty)_\chi \cong (\varprojlim \mu_{p^n})_\chi$.

Assume that $\chi = \omega$. Then $(E_\infty)_\omega \cong \varprojlim \mu_{p^n}$, and the natural mapping $\varprojlim \mu_{p^n} \rightarrow \bigoplus_{q \in S_\omega} R_q$ is injective. We also note that $d_\omega = 1$. From these facts, we see that

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\omega = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\omega + \sum_{q \in S_\omega} \text{rank}_{\mathbb{Z}_p} (R_q)_\omega - 1 = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\omega + \sum_{q \in S_\omega} p^{m_q} - 1.$$

Assume that χ is odd and $\chi \neq \omega$. Then $(E_\infty)_\chi$ is finite. (In general, it may be non-trivial. See [12].) Hence we see

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} d_\chi p^{m_q}.$$

Let ε be the trivial character. Then we can see that

$$X_S(K_\infty)_\varepsilon \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong X_S(\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \quad X(K_\infty)_\varepsilon \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong X(\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

by using Lemma 2.1 of [4]. Hence $\text{rank}_{\mathbb{Z}_p} X(K_\infty)_\varepsilon = 0$. We also note that

$$S_\varepsilon = \{q \in S \mid \omega(\sigma_{0,q}) = 1\} = \{q \in S \mid q \equiv 1 \pmod{p}\}.$$

By the results for \mathbb{Q}_∞ (see [5]), we see that $X_S(\mathbb{Q}_\infty) = X_{S_\varepsilon}(\mathbb{Q}_\infty)$, and

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\varepsilon = \sum_{q \in S_\varepsilon} p^{m_q} - \max\{p^{m_q} \mid q \in S_\varepsilon\}.$$

Since $d_\varepsilon = 1$ and $f_{q,\varepsilon} = (1+T)^{p^{m_q}} - \kappa_0^{p^{m_q}}$, we see that

$$\max\{p^{m_q} \mid q \in S_\varepsilon\} = d_\varepsilon \deg F(T).$$

From these facts, the formula

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\varepsilon = X(K_\infty)_\varepsilon + \sum_{q \in S_\varepsilon} d_\varepsilon p^{m_q} - d_\varepsilon \deg F(T)$$

is certainly satisfied.

Finally, assume that χ is non-trivial and even. By Proposition 6.3, we see that

$$(E_\infty)_\chi / f_{q,\chi}(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is an isomorphism. This isomorphism implies that

$$(E_\infty)_\chi / F(T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \rightarrow \bigoplus_{q \in S_\chi} (R_q)_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is injective. By using the same argument stated in the proof of Proposition 6.3, we obtain that $\dim_{\mathbb{Q}_p}(\mathcal{E}_\chi / F(T)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = d_\chi \deg F(T)$. Hence we see that

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} d_\chi p^{m_q} - d_\chi \deg F(T).$$

We have shown the formula for all cases. \square

Remark. Assume that p does not divide $|G|$. Then $f_{q,\chi}(T) = (1+T)^{p^{m_q}} - \kappa_0^{p^{m_q}}$, and hence $\deg F(T) = \max\{p^{m_q} \mid q \in S_\chi\}$. Moreover, we can see that p^{m_q} is equal to the number of primes of \mathbb{Q}_∞ lying above q .

Example 6.5. We put $K = \mathbb{Q}(\mu_p)$, the p th cyclotomic field (recall that p is an odd prime). In this case, every character of $G = \text{Gal}(K/\mathbb{Q})$ is written by the form ω^i with $0 \leq i \leq p-2$. Note also that $q \in S$ is unramified in K . We may identify G with $(\mathbb{Z}/p\mathbb{Z})^\times$, and $\sigma_{0,q}$ with $q \pmod{p}$. Then we can see

$$S_{\omega^i} = \{q \in S \mid \omega^{1-i}(\sigma_{0,q}) = 1\} = \{q \in S \mid i \equiv 1 \pmod{f_q}\},$$

where f_q is the order of q in $(\mathbb{Z}/p\mathbb{Z})^\times$. Assume that S_{ω^i} is not empty. We put

$$P^{(i)} = \begin{cases} 1 & (i = 1) \\ 0 & (i : \text{odd}, i \neq 1) \\ \max\{p^{m_q} \mid q \in S_{\omega^i}\} & (i : \text{even}). \end{cases}$$

By Theorem 6.4, we see

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_{\omega^i} = \lambda_{\omega^i} + \sum_{q \in S_{\omega^i}} p^{m_q} - P^{(i)},$$

where $\lambda_{\omega^i} = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_{\omega^i}$ is the ω^i -part of the (unramified) Iwasawa λ -invariant of K_∞/K .

Example 6.6. Let k be a real quadratic field with conductor d (the case that p divides d is allowed). We put $K = k(\mu_p)$. Let χ be the quadratic character of $G = \text{Gal}(K/\mathbb{Q})$ corresponding to k . We may regard χ (resp. ω) as a Dirichlet character modulo d (resp. modulo p). In this case, we see

$$S_\chi = \{q \in S \mid \chi(q) \neq 0, \chi(q) = \omega(q)\}.$$

Hence S_χ consists of the primes in S which satisfy:

- $q \equiv 1 \pmod{p}$ and q splits in k , or
- $q \equiv -1 \pmod{p}$ and q is inert in k .

Assume that $S_\chi \neq \emptyset$. We put $P = \max\{p^{m_q} \mid q \in S_\chi\}$, then we obtain the formula

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + \sum_{q \in S_\chi} p^{m_q} - P.$$

Note that $\text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi$ is equal to the (unramified) Iwasawa λ -invariant of k_∞/k . (If Greenberg's conjecture is true for k and p , then $\text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi = 0$.) Since

$$X_S(k_\infty) \cong X_S(K_\infty)_\chi \oplus X_{S_\varepsilon}(\mathbb{Q}_\infty)$$

(where ε is the trivial character), we can compute the \mathbb{Z}_p -rank of $X_S(k_\infty)$.

Example 6.7. Let F/\mathbb{Q} be a cyclic extension of degree p . Assume that p is unramified in F . We put $K = F(\mu_p)$, and fix a character χ of $G = \text{Gal}(K/\mathbb{Q})$ satisfying $K^{\ker(\chi)} = F$. Let σ be a fixed generator of $\text{Gal}(F_\infty/\mathbb{Q}_\infty) \cong \text{Gal}(F/\mathbb{Q})$, and $F^{(i)}$ the fixed field of F_∞ by $\langle \gamma\sigma^i \rangle$ for $0 \leq i \leq p-1$ (hence $F^{(0)} = F$). For simplicity, we assume that every prime of S is not decomposed in \mathbb{Q}_∞ . Hence if $q \in S$ is unramified in F , then the splitting field of F_∞/\mathbb{Q} for q must be one of $F^{(0)}, \dots$, or $F^{(p-1)}$. By the definition of χ , we see that $\chi^{-1}(\sigma)$ is defined, and we put $\chi^{-1}(\sigma) = \zeta$ (note that ζ is a primitive p th root of unity). In this case, we obtain that

$$S_\chi = \{q \in S \mid q \equiv 1 \pmod{p}, q \text{ is not ramified in } F\}.$$

Under the assumption for S , we see $m_q = 0$ for all $q \in S_\chi$. When $q \in S_\chi$ splits in $F^{(i)}$, we see that $\chi^{-1}(\sigma_{p,q}) = \chi^{-1}(\sigma^i) = \zeta^i$, and hence $f_{q,\chi}(T) = (1+T) - \zeta^i \kappa_0$. We note that if $i \neq j$, then $(1+T) - \zeta^i \kappa_0$ and $(1+T) - \zeta^j \kappa_0$ are relatively prime. We put

$$S_{\chi,i} = \{q \in S_\chi \mid q \text{ splits in } F^{(i)}\},$$

for $0 \leq i \leq p-1$. Assume that $S_\chi \neq \emptyset$. From the above facts, we see that $\deg F(T)$ is equal to the number of non-empty $S_{\chi,i}$'s. That is,

$$\deg F(T) = |\Psi|, \text{ where } \Psi = \{i \mid 0 \leq i \leq p-1, S_{\chi,i} \neq \emptyset\}.$$

Since $d_\chi = p-1$, we see

$$\text{rank}_{\mathbb{Z}_p} X_S(K_\infty)_\chi = \text{rank}_{\mathbb{Z}_p} X(K_\infty)_\chi + (p-1) \sum_{i \in \Psi} (|S_{\chi,i}| - 1).$$

Acknowledgement. The main idea of the present paper is due to the previous paper [5]. The author express his thanks to Professors Yasushi Mizusawa and Manabu Ozaki for giving many suggestions during (and after) the collaborative work. The author was supported by Research Grant of Research Institute of Chiba Institute of Technology.

REFERENCES

- [1] A. Brumer : *On the units of algebraic number fields*, Mathematika, **14** (1967), 121–124.
- [2] R. Greenberg : *On a certain ℓ -adic representation*, Invent. Math., **21** (1973), 117–124.
- [3] R. Greenberg : *On p -adic L -functions and cyclotomic fields. II*, Nagoya Math.J., **67** (1977), 139–158.
- [4] C. Greither : *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier (Grenoble), **42** (1992), 449–499.
- [5] T. Itoh, Y. Mizusawa, M. Ozaki : *On the \mathbb{Z}_p -ranks of tamely ramified Iwasawa modules*, arXiv:1103.3916, (2011).
- [6] K. Iwasawa : *On \mathbb{Z}_l -extensions of algebraic number fields*, Ann. of Math. (2), **98** (1973), 246–326.
- [7] K. Iwasawa : *Riemann-Hurwitz formula and p -adic Galois representations for number fields*, Tôhoku Math. J., **33** (1981), 263–288.
- [8] C. Khare, J.-P. Wintenberger : *Ramification in Iwasawa modules*, arXiv:1011.6393, (2010).
- [9] Y. Mizusawa, M. Ozaki : *On tame pro- p Galois groups over basic \mathbb{Z}_p -extensions*, preprint.
- [10] : J. Neukirch, A. Schmidt, K. Wingberg : *Cohomology of number fields*, Second edition, Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, Heidelberg, 2008.
- [11] L. Salle : *On maximal tamely ramified pro-2-extensions over the cyclotomic \mathbb{Z}_2 -extension of an imaginary quadratic field*, Osaka J. Math., **47** (2010), 921–942.
- [12] T. Tsuji : *Semi-local units modulo cyclotomic units*, J. Number Theory, **78** (1999), 1–26.
- [13] L. C. Washington : *Introduction to cyclotomic fields*, Second edition, Graduate texts in mathematics **83**, Springer-Verlag, New York, Berlin, Heidelberg, 1996.

Tsuyoshi Itoh

Division of Mathematics, Education Center, Faculty of Social Systems Science, Chiba Institute of Technology, 2-1-1 Shibazono, Narashino, Chiba 275-0023, Japan
e-mail : tsuyoshi.itoh@it-chiba.ac.jp